Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] What is claimed is:

1. An inverse key evaluation circuit for a crypto-system, the inverse key evaluation circuit comprising:

a key-receiving module comprising an N-bit register which comprises m groups of registers for receiving an N-bit key which comprises m groups of keys, the m groups of keys stored in the m groups of registers respectively, both of N and m being power-of-two integers larger than two; and

an inverse key evaluation module comprising m XOR logic gates and a digital data processing module for inversely evaluating to generate a plurality of pre-keys in sequence according to the keys received by the key-receiving module;

wherein the keys stored in the N-bit register are replaced in sequence by the pre-keys which are obtained by utilizing the inverse key evaluation module to process the keys once.

[c2] 2.The inverse key evaluation circuit of claim 1 wherein the value of N is 128 and the value of m is 4, the key received by the key-receiving module at first is inverse

evaluated ten times to generate ten pre-keys in order.

[c3] 3. The inverse key evaluation circuit of claim 1 wherein the digital data processing module in the inverse key evaluation module is electrically connected to the m XOR logic gates, the digital data processing module comprising:

a byte rotator for inverting the order of a plurality of bytes in the N-bit key;

a byte substituter electrically connected to the byte rotator for substituting a plurality of predetermined bytes for the bytes in the N-bit key; and

a byte disturber for generating a disturbing value according to a predetermined disturbing table and utilizing the disturbing value to perform an XOR operation with the bytes in the N-bit key.

[c4] 4.The inverse key evaluation circuit of claim 1 wherein the inverse key evaluation circuit further comprises a register electrically connected to the inverse key evaluation module for storing a key obtained through one inverse key evaluation, wherein the key storing in the register is replaced by a pre-key generated from the key through one inverse key evaluation.

[c5] 5.The inverse key evaluation circuit of claim 1 wherein the crypto-system is qualified to an advanced encryption

standard (AES).

[c6] 6.The inverse key evaluation circuit of claim 5 wherein the crypto-system is applied to a wireless LAN.

[c7] 7.A decrypting method for decrypting an N-bit enciphered text string to a corresponded N-bit plain text string, N being a power-of-two integer larger than two, the decrypting method comprising:
providing a key and the enciphered text string;
utilizing an inverse key evaluation module to sequentially generate a plurality of pre-keys of the key; and
using the key and the pre-keys generated from the key to perform a plurality of corresponding decryption operations for decrypting the enciphered text string to the plain text string.

[c8] 8. The method of claim 7 wherein the method further comprises using a register to store the key and the pre-keys sequentiallygenerated from the key, the key stored in the register is sequentially replaced by a next pre-key which is obtained by utilizing the inverse key evaluation module to process the key once.

[c9] 9. The method of claim 7 wherein the key is a N-bit key, in which N is equal to 128, and 10 pre-keys can be obtained in order from the key via the inverse key evalua-

tion module.

[c10] 10. The method of claim 9 wherein the inverse key evaluation module comprises m XOR logic gates and a digital data processing module to perform a plurality of inverse key evaluations according to the key and sequentially generate a plurality of pre-keys corresponding to the key, m being a power-of-two integer larger than two.

[c11] 11. The method of claim 10 wherein the digital data processing module is electrically connected to the m XOR gates, the digital data processing module comprising:
a byte rotator for inverting the order of a plurality of bytes in the N-bit key;
a byte substituter electrically connected to the byte rotator for substituting a plurality of predetermined bytes for the bytes of the N-bit key; and
a byte disturber for generating a disturbing value according to a predetermined disturbing table and utilizing the disturbing value to perform an XOR operation with the bytes in the N-bit key.

[c12] 12. The method of claim 7 wherein the method is qualified to an advance encryption standard (AES).

[c13] 13.The method of claim 12 wherein the method is applied to a crypto-system in a wireless LAN.

[c14] 14. A crypto-system for performing a plurality of encryption operations and a plurality of decryption operations, the crypto-system comprising:
a key-generating module for providing a plurality of keys, the key-generating module comprising:
a forward key evaluation circuit for generating a plurality of post-keys of an original key according to the original key until generating the last key;
an inverse key evaluation circuit for generating a plurality of pre-keys of the last post key according to the last post-key until generating the original key; and
at least one register for storing the original key and the last post-key;
an encryption module electrically connected to the key-generating module for sequentially performing a plurality of corresponding encryption operations according to the original key and the post-keys sequentially generated, which are provided by the forward key evaluation circuit, to encrypt a plain text string to a corresponding enciphered text string; and
a decryption module electrically connected to the key-generating module for sequentially performing a plurality of corresponding decryption operations according to the last post-key and the pre-keys sequentially generated, which are provided by the inverse key evaluation

circuit, to decrypt an enciphered text string to a corresponding plain text string.

[c15] 15. The crypto-system of claim 14 wherein the encryption module is a ROM-based encryption module comprising a plurality of ROMs for storing algorithms corresponding to the plurality of encryption operations and related application programs.

[c16] 16. The crypto-system of claim 14 wherein the plain text string, the enciphered text string, and the plurality of keys are all 128-bit digital data.

[c17] 17. The crypto-system of claim 14 wherein the inverse key evaluation circuit comprises:
a key-receiving module for receiving the last key;
an inverse key evaluation module comprising a plurality of XOR logic gates and a digital data processing module for generating a plurality of pre-keys according to the last key received by the key-receiving module until generating the original key; and
a register electrically connected to the inverse key evaluation module for storing a key obtained through one inverse key evaluation, the key stored in the register replaced by a pre-key obtained from the key through one inverse key evaluation.

[c18] 18. The crypto-system of claim 14 wherein the crypto-system is qualified to an advance encryption standard (AES).

[c19] 19. The crypto-system of claim 18 wherein the crypto-system is applied to a wireless LAN.